PATENT
Attorney Docket No.: NVDA/P000736

UNITED STATES PATENT APPLICATION FOR:

METHOD AND APPARATUS FOR CONTENT PROTECTION

INVENTORS:

IAN M. WILLIAMS
MICHAEL B. DIAMOND

ATTORNEY DOCKET NUMBER: NVDA/P000736

CERTIFICATION OF MAILING UNDER 37 C.F.R. 1.10

I hereby certify that this New Application and the documents referred to as enclosed therein are being deposited with the United States Postal Service on Oct 22, 03, in an envelope marked as "Express Mail United States Postal Service", Mailing Label No. EV413805545US, addressed to: Commissioner for Patents, Mail Stop PATENT APPLICATION, P.O. Box 1450, Alexandria, VA 22313-1450

Alberta Gamble
Signature

ALBERTA GAMBLE
Name

10/22/03
Date of signature

MOSER, PATTERSON & SHERIDAN LLP
595 Shrewsbury Ave.
Shrewsbury, New Jersey 07702
(732) 530-9404

METHOD AND APPARATUS FOR CONTENT PROTECTION

FIELD OF THE INVENTION

[0001] One or more aspects of the invention relate generally to protection of content, and more particularly to a content protection environment.

BACKGROUND OF THE INVENTION

[0002] Content protection may be cryptographically based or signal-processing based or a combination thereof. Generally, cryptographically-based content protection is applied to the digital domain, while signal-processing based content protection is applied to the analog domain.

[0003] There are many examples of cryptographically-based content protection in use today. Digital video discs ("DVDs") use a Content Scrambling System ("CSS") that requires a 40-bit long key to decipher the encrypted content. Content Protection for Recordable Media ("CPRM") is a broadcast encryption technology applied to physical media, where a media key block is prerecorded on blank media. Content Protection for Pre-recorded Media, a variant of CPRM, is used to protect DVD Audio formatted discs. CPRM is also used to protect content stored in Secure Digital Memory Cards, Secure CompactFlash, the IBM MicroDrive, and DVD video recorders.

[0004] More recent developments include Digital Transmission Content Protection ("DTCP"), a public-key technology applied to a digital bus, such as a Universal Serial Bus ("USB") and an Institute of Electronic and Electrical Engineers ("IEEE") 1394 bus ("Firewire"). High Definition Content Protection ("HDCP") has been proposed to protect content transferred from a Digital Video Interface ("DVI") (a digital video interface to a high-definition monitor/television). HDCP expands on authentication of DTCP to establish a session key used to encrypt video data.

[0005] In the software arena, content protection includes cryptographic switching ("cryptoswitch") and digital signets technologies. Cryptoswitch involves only having a small portion of a program in the clear for runtime, and leaving the remainder encrypted. Signets are used to detect unauthorized

modification of a program.

[0006] The standards bodies of Digital Video Broadcast and TV Anytime have considered proposals for content protection in home networks, such as SmartRight, Open Conditional Content Access Management ("OCCAM") and xCP Cluster Protocol. Other network or system level approaches include Broadcast Flag, Content Protection System Architecture ("CPSA") and Digital-Rights Management ("DRM") systems. In Broadcast Flag, a bit is set to indicate content is not to be distributed over the Internet, and otherwise the content is protected by DTCP and CPRM. CPSA is another architecture describing how DTCP and CPRM fit together along with watermarking, using interlocking licenses. DRM systems use the Internet to distribute keys for decryption through a clearing house.

[0007] In the signal-processing based content protection arena, an out-of-specification television signal, not detectible by a television, but detectable by most video recorders is used. Also, digital watermarking for copy control, whether record control or playback control, is used. Pattern recognition ("fingerprinting") is being considered. However, recognition is a statistical process, which by definition, is inexact. A library of content needing to be interrogated would be significantly large, for example for broadcast monitoring. Accordingly, watermarking is presently more favored for identification purposes.

[0008] Because of the many ways that content may be copied, displayed and distributed, no one technology is a complete solution to protecting content within all of these possible contexts. Accordingly, technology that advances the interests of a content protection environment is desirable and useful.

SUMMARY OF THE INVENTION

[0009] An aspect of the invention is a method for protecting digital content. The digital content is provided to a graphics processor. A portion of the frames of the digital content is altered at least approximately contemporaneous with recording within the graphics processor responsive to tags in a data stream provided thereto, where alteration of the portion of the frames of the digital content is not visually perceptible for real-time display but is visually perceptible in recorded version thereof.

[0010] An aspect of the invention is a device for protecting digital content, comprising a graphics processor configured to detect tags in a data stream and to associate the tags detected with commands for altering image content.

[0011] An aspect of the invention is digital video content, comprising: tags for altering frames by a graphics processor.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Accompanying drawing(s) show exemplary embodiment(s) in accordance with one or more aspects of the invention; however, the accompanying drawing(s) should not be taken to limit the invention to the embodiment(s) shown, but are for explanation and understanding only.

[0013] FIG. 1 is a high-level block diagram depicting an exemplary embodiment of a compute.

[0014] FIG. 2 is a high-level block diagram depicting an exemplary embodiment of a digital image, still or moving, camera.

[0015] FIG. 3 is a high-level block diagram depicting an exemplary embodiment of a recorder, such as a compact disc ("CD") or DVD recorder, for recording digital information.

[0016] FIG. 4 is a high-level block diagram depicting an exemplary embodiment of a monitor, such as for a high-definition television ("HDTV") or a computer, for displaying digital information.

[0017] FIGS. 5A through 5E are respective pictorial diagrams of an image for a sequence of frames.

[0018] FIG. 6 is a high-level block diagram depicting an exemplary embodiment of a graphics pipeline.

[0019] FIG. 7 is a block diagram depicting an exemplary embodiment of an image content distortion system.

[0020] FIG. 7A is a block diagram depicting an exemplary embodiment of an alternate embodiment of an image content distortion system.

[0021] FIG. 8 is a block diagram depicting an exemplary embodiment of an image content protection system.

[0022] FIGS. 9A and 9B are pictorial diagrams of an example of a display environment.

[0023] FIGS. 10A and 10B are pictorial diagrams of an example of another display environment.

[0024] FIGS. 11A and 11B are pictorial diagrams of an example of a record environment.

[0025] Figure 12 illustrates a graphical user interface for entry of key information.

DETAILED DESCRIPTION OF THE DRAWINGS

[0026] The description that follows is directed to image cloaking and watermarking for a content protection environment or an enhanced content protection environment. The image cloaking may be embedded in the content itself, the recording device, the driver software, or the hardware, or any combination of one or more of the above. Content is cloaked without disturbing the viewing experience for authorized users. A rendering unit ("RU") is used to process video data to provide image cloaking. Examples of rendering units include graphics processing units (GPU) and video processing units (VPU).

[0027] FIG. 1 is a high-level block diagram depicting an exemplary embodiment of a computer 100. Computer 100 includes at least one microprocessor 101, an input/output ("I/O") interface 102, system memory 105, a RU 103 and optionally RU memory 104. Image information provided to RU 103 is cloaked by RU 103.

[0028] FIG. 2 is a high-level block diagram depicting an exemplary embodiment of a digital image, still or moving, camera 200. Visual information is obtained via lens 201 which is provided to charge-coupled device ("CCD") 202. The visual information is converted from its analog form to a digital representation thereof by CCD 202. The digital representation is provided to RU 203 for processing. Output of RU 203 is provided to a transducer 204 for writing to media 205 in an embodiment. In another embodiment, transducer 204 is omitted for writing to media 205, where media is a direct storage means, such as flash memory, among other direct digital information storage means.

[0029] FIG. 3 is a high-level block diagram depicting an exemplary embodiment of a recorder 300, such as a compact disc ("CD") or DVD recorder, for recording digital information. Digital information 304 obtained from a source, such as

broadcast, Internet download, original content CD or DVD, videotape, and the like, is provided to RU 303 for processing. Output of RU 303 is provided to transducer 301 for writing to media 302. In another embodiment, transducer 301 is omitted for writing to media 302, where media is a direct storage means, such as flash memory, among other direct digital information storage means.

[0030] FIG. 4 is a high-level block diagram depicting an exemplary embodiment of a monitor 400, such as for a high-definition television ("HDTV") or a computer, for displaying digital information. Digital information 404 obtained from a source, such as broadcast, Internet download, original content CD or DVD, videotape, and the like, is provided to RU 403 for processing. Output of RU 403 is provided to transducer 401 for displaying on display screen 402. Notably, a projector 410 may be used with a separate surface for imaging.

[0031] Prior to a detailed description the above-mentioned RUs, a pictorial description of results from such RUs is provided for clarity.

[0032] FIGS. 5A through 5E are respective pictorial diagrams of an image 500 for a sequence of frames. In its unadulterated state in FIG. 5A, image 500 for a frame in a sequence includes a picture 501, a desk 502, a person 503 and a filing cabinet 504. However, in a next or subsequent frame in the sequence of frames, a part of the scene, such as filing cabinet 504, may be removed, as shown in FIG. 5B. In a next or subsequent frame in the sequence of frames, a part of the scene, such as filing cabinet 504, may be moved and a character, such as person 503, may be removed, as shown in FIG. 5C. Additionally or alternatively, an addition of an object, such as a text message or a character, may be added to a scene. For example, as shown in FIG. 5D, a text message 511 and a character 512 have been added to image 500. Furthermore, inserted objects may be may be inserted at different locations from frame-to-frame, as shown in FIG. 5E with respect to text message 511 and character 512.

[0033] Thus, it should be appreciated that image processing may include adulteration of source material by one or more of the following: insertion of one or more objects that are not part of the source material, movement of one or more inserted objects that are not part of the source material, movement of one or more objects that are part of the source material, removal ("cloaking") of one

or more objects of the source material. Additionally, a RU, responsive to detected watermarking of source material or requesting of key for the source material, may invoke adulteration unless a proper response is provided. It should be appreciated that prior attempts at cloaking video have involved prerecorded changes. Prerecorded changes are more easily defeated than real-time randomly imposed changes to source material.

[0034] FIG. 6 is a high-level block diagram depicting an exemplary embodiment of a graphics pipeline 600. Graphics pipeline 600 is shown as an OpenGL pipeline for purposes of clarity by example; however, any of a variety of known pipeline architectures may be used. Graphics pipeline 600 may be in any of the above-mentioned RUs 103, 203, 303, and 403. Image information or content, and commands, 601 are provided to Graphics pipeline 600 with frame dividers and with tags for video cloaking. Graphics pipeline 600 includes display list stage 602, evaluator stage 603, per-vertex operations and primitive assembly stage 604, pixel operations stage 605, rasterization stage 606, texture memory stage 607, per-fragment operations stage 608, and frame buffer stage 609.

[0035] FIG. 7 is a block diagram depicting an exemplary embodiment of an image content distortion system 700. Notably, video protection system may be partially or completely internal within a RU. Optionally, a decryptor 710 is included with image content distortion system for decrypting a received encrypted command and data stream 711 and providing a decrypted command and data stream 701. A pop-up graphical user interface ("GUI") may be displayed by a RU responsive to detecting encrypted content, where the GUI has a data entry block for entry of a key by a user. Command and data stream 701 is provided to buffer 702 and to tag detector 703. Tags in command and data stream 701 are detected by tag detector 703, and detected tags are provided to action table 704.

[0036] Action table 704 may be a lookup table with tags and associated commands. Thus, a detected tag may be used to find an associated command in action table 704. Tags and associated commands may be predefined as part of video protection system 700, or, alternatively or in combination, tags and associated commands may be selected and programmed into action table 704.

[0037] A found command ("tagged command") in action table 704 may then optionally be provided to a randomizer, to randomly apply ignore or send a received tagged command to buffer 702. A randomizer may be used for difficulty in filtering out video display results associated with tagged commands, as well as for reducing possibility of negatively impacting viewing of video display results. Randomizer 705 may include a random number generator. Alternatively, randomizer 705 may include a counter, for example to count each watermark tag, or command therefor, and to insert watermarks after each count of some number of such watermark tags or to alter the image content responsive to watermark count. Furthermore, in response to detection of one or some number of watermark tags, a GUI may be invoked for a user to enter a key. For example, Figure 12 illustrates a graphical user interface having key information. Responsive to entry of an acceptable key being entered, a user may be provided access to a highest quality of resolution allowed or some down sampled version thereof. Alternatively, responsive to an acceptable key not being entered a low quality image may be displayed. In another embodiment, an acceptable key may be used to toggle video cloaking off, or to toggle recording on.

[0038] Buffer 702 stores data and associated command information, and thus tagged commands may be stored back in the same association in which the tags for the tagged commands were received.

[0039] Tagged commands associated with texture may include blending commands for cloaking image content or blocking commands for inserting image content, such as an image overlay or underlay. Thus, for example, both blending and blocking may be used simultaneously with respect to the same frame of image content.

[0040] Tagged commands for blocking may obtain predefined textures from a separate over/underlay memory 706, which in response may provide a selected overlay/underlay to buffer 702 for temporary storage, or optionally directly to graphics pipeline 600, such as for texture memory 607 of FIG. 6. Notably, this technology may be used in two-dimensional rendering, as well as three-dimensional rendering. For three-dimensional rending, display lists may be

used for processing image content with tagged commands.

[0041] Accordingly, it should be understood that image content may be inserted, deleted and modified. Furthermore, it is not necessary that insertions be added into image content, but may be inserted into a vertical blanking interval.

[0042] Cloaking is done using tags inserted into a command/data stream. Each tag indicates a starting and ending location. For example, a starting and ending vertex may be identified. Also, by way of example, a starting and ending texel may be identified. It is not necessary to explicitly identify an ending location. For example, a starting vertex of a tri-strip may be identified, and a set number of triangles may be set for cloaking starting from that starting vertex.

[0043] Furthermore, this technology may be used for affecting visual content to display image content with different ratings. For example, an R rated movie due to nudity, may be displayed as a PG movie without nudity by adding cloaking responsive to tagging the image content. This type of cloaking may involve adding image content for blocking nudity, or may involve distorting image content, such as use of a magnified portion of the image to blur a pixel ("pixelation").

[0044] Additionally, tags may be used to set the refresh rate. By varying the refresh rate, unauthorized copiers would get a distorted copy.

[0045] Notably, tags do not need to be explicitly identified. Tags may be particular vertices or a combination of multiple vertices. For example, if two, or some other number greater than two, vertices in a row have a particular dot product value, that value may be used as a tag. There may be one or more values that are used as tags. Accordingly, a tag detector for this example would take dot products and compare them bitwise to one or more dot product tags. Additionally, a particular geometry may be tagged, such as a body part of a character, for cloaking, and such geometry could be cloaked responsive. Furthermore, it may be one polygon that is used to provide a tag. Moreover, it may be a plurality of vertices of a plurality of associated polygons not necessarily connected to one another that are used to provide a tag.

[0046] Furthermore, for three dimensional renderings, each display list may be identified for cloaking or no cloaking of image content. Thus, a tag may be used

to indicate which display lists will be cloaked.

[0047] Furthermore, it should be appreciated that image content is includes video or graphically generated content, and is not limited to movies or other forms of moving pictures, but may include computer aided design content. Additionally, such content may be displayed without significantly impacting the viewing experience, while significantly impacting the viewing experience of unauthorized copies.

[0048] FIG. 7A is a block diagram depicting an exemplary embodiment of an alternate embodiment of an image content distortion system 700. In this embodiment, randomizer 705 is coupled to tag detector 703 to obtain an indication of when tags are detected. Responsive to detecting a tag, randomizer 705 randomly activates action table 704 to carry out a command associated with a detected tag.

[0049] FIG. 8 is a block diagram depicting an exemplary embodiment of an image content protection system 800. Image content protection system 800 is similar to image distortion system 700 of FIG. 7, except that tag detector 703 is replaced with tag detector/decryptor 803. For systems where command and data stream 701 is not encrypted over a bus prior to being received by a RU, detector/decryptor 803 detects and decrypts tags. A decrypted tag may be used as described above.

[0050] Another use for tags is to provide for one of a plurality of levels of image resolution. Thus, fully authorized use, would be a highest available resolution, where a less than fully authorized use would be for a down-sampled version of the highest available resolution for display device 810 coupled to image content protection system. Furthermore, unauthorized use, such as no encrypted tag to decrypt, may distort the viewing experience. For example, each frame location may be moved unless proper authorization is received.

[0051] Furthermore, content received having a watermark may be detected based on the watermark. Watermarked content may be down-sampled unless an authorization code is provided.

[0052] Accordingly, it should be appreciated that image data may be added, removed or modified to provide cloaked image content. One or more tags may

be used on each frame to clock image data. To avoid significantly impacting authorized viewing experience, cloaked image content is done on only on selected objects of selected frames, which selection may be randomly imposed.

[0053] Additionally, forms of cloaking may be content provider specific. Action table 704 may further be indexed to content providers, such that a subset of all available cloaking applications is used.

[0054] FIGS. 9A and 9B are pictorial diagrams of an example of a display environment 900. Image 500 is displayed by projector 410, and appears to viewers as shown in FIG. 9A. However, because projector 410 is as described above, image 500 as it appears to camera 902 is recorded with overlays 511 and 512 (labeled in FIG. 5D) as shown in FIG. 9B. If three-dimensional processing is used to provide image 500, items may be removed as described above.

[0055] FIGS. 10A and 10B are pictorial diagrams of an example of a display environment 1000. Image 500 is provided from image content source 1001. If image content source 1001 includes tags as described above, monitor 400 will produce a protected content version responsive to such tags. For example, image 500 appears to viewers as shown in FIG. 10A. However, because monitor 400 is as described above, image 500 as it appears to camera 902 is recorded with overlays 511 and 512 (labeled in FIG. 5D) as shown in FIG. 10B. If three-dimensional processing is used to provide image 500, items may be removed, added or modified as described above.

[0056] FIGS. 11A and 11B are pictorial diagrams of an example of a record environment 1200. Image 500 is provided from an image content source to a monitor 1201. Image 500 appears to viewers as shown in FIG. 11A. However, because recorder 300 is as described above, image 500 as recorded by recorder 300 for playback is recorded with overlays 511 and 512 (labeled in FIG. 5D) as shown in FIG. 11B. If three-dimensional processing is used to provide image 500, items may be removed, added or modified as described above.

[0057] Some embodiments of the present invention make use of key information to enable specific features. Figure 12 illustrates a computer display 1200

having a graphical user interface 1202 that includes a data entry box 1204. In operation, a user will enter a key in the data box 1204 and then cause that key information to be input to an underlying software routine. Such manual entry of information is well-known and is widely supported in software development programs. Once the key is obtained by software, that software compares the key information with a key data list. If the entered key is deemed acceptable, that is, the entered key is on the key data list, the locked-out features are made available to the operator.

[0058] While the foregoing describes exemplary embodiment(s) in accordance with one or more aspects of the invention, other and further embodiment(s) in accordance with the one or more aspects of the invention may be devised without departing from the scope thereof, which is determined by the claim(s) that follow and equivalents thereof. Claim(s) listing steps do not imply any order of the steps. Trademarks are the property of their respective owners.